

CLAIMS

What is claimed is:

1. A method, comprising:
receiving a plurality of reports from a community of users, each report identifying an email message as spam or not spam; and
determining if the email message is spam based on a number of the reports received from the community of users, and a trust factor associated with each user.
2. The method of claim 1, further comprising maintaining a database of email messages determined as being spam.
3. The method of claim 2, further comprising providing notifications to the community of users of email messages stored in the database and determined as being spam.
4. The method of claim 3, wherein each notification is in response to a request received from a user in the community for an indication on whether an identified message is spam.
5. The method of claim 1, wherein each report comprises at least one signature based on a content of the email message.

6. The method of claim 1, wherein the trust factor is based on an indication of how accurately previous reports sent by the user identified email messages as spam.

7. A server, comprising:

a processor; and

a memory coupled to the processor, the memory storing instructions which when executed by the processor cause the processor to perform a method, comprising:

receiving a plurality of reports from a community of users, each report identifying an email message as spam or not spam; and

determining if the email message is spam based on a number of the reports received from the community of users, and a trust factor associated with each user.

8. The server of claim 7, wherein the method further comprises maintaining a database of email messages determined as being spam.

9. The server of claim 8, wherein the method further comprises providing notifications to the community of users of email messages stored in the database and determined as being spam.

10. The server of claim 9, wherein each notification is in response to a request received from a user in the community for an indication on whether an identified message is spam.

11. The server of claim 7, wherein each report comprises at least one signature based on a content of the email message.

12. The server of claim 7, wherein the trust factor is based on an indication of how accurately previous reports sent by the sender identified email messages as spam.

13. A computer-readable medium having stored thereon a sequence of instructions which when executed by a computer, cause the computer to perform a method comprising:

receiving a plurality of reports from a community of users, each report identifying an email message as spam or not spam; and

determining if the email message is spam based on a number of the reports received from the community of users, and a trust factor associated with each user.

14. The computer-readable medium of claim 13, wherein the method further comprises maintaining a database of email messages determined as being spam.

15. The computer-readable medium of claim 14, wherein the method further comprises providing notifications to the community of users of email messages stored in the database and determined as being spam.

16. The computer-readable medium of claim 15, wherein each notification is in response to a request received from a user in the community for an indication on whether an identified message is spam.

17. The computer-readable medium of claim 13, wherein each report comprises at least one signature based on a content of the email message.

18. The computer-readable medium of claim 14, wherein the trust factor is based on an indication of how accurately previous reports sent by the sender identified email messages as spam.